Exhibit A

Virginia House of Delegate
APPROPRIATE USE POLICY

The following defines the computer use policy for the Virginia House of Delegates, as originally developed by the Joint Rules Committee in January, 2002. This policy governs the use of state-owned personal computers and House technology resources assigned to legislators for accessing House of Delegates and Virginia General Assembly systems.

Information Access Policy

The Virginia House of Delegate maintains public and private information on our computer system. This requires adherence to many rules regarding access to information. A brief outline of some basic rules follows:

House Information Systems operates in a position of trust regarding various materials to provide management support. To perform effectively, they must be able to gain access to all computers with the guarantee that this access is used only for authorized purposes with the employees' knowledge, to the extent possible, and under the following conditions:

1. For problem resolution
2. To retrieve network information
3. For computer backups
4. To determine unauthorized computer use
5. To complete FOIA and legal research requests

Any information or software stored on any computer system maintained by this agency is subject to all laws regarding access, disclosure, and copyright protection. As employees of the Commonwealth, we serve the public and are accountable for our actions regarding software or information access (see Software Regulation).

Information developed for or concerning a member of the House of Delegates will be released only upon written request to the Clerk of the House of Delegates

Prototypes created for the House of Delegates are the property of the House of Delegates.

Any House of Delegates computers, phones and tablets are subject to the Freedom of Information Act. Staff must use discretion to assure that all software used is legal. The Clerk may at any time ask Information Systems to explore suspected unauthorized use.

Additional Computers and Equipment Connected to the House Network

Many members wish to have additional computers on the House network in their legislative assistants' offices. Members can connect one additional computer to the secure House network, and add any other computers via our public wireless network. Computers accessing the internet via public wireless can access any website, but will not have access to member shared drives on the House server, or access to printers on the House network.

Second computers that are connected to the secure House network need to be evaluated by House Information systems staff prior to gaining login credentials. Although most PCs can be connected to our network, House Information Systems cannot guarantee the successful configuration of all second computers. **Only network hardware provided by the House can be used to connect additional computers to the House network.**

Due to the large number of viruses that cause serious problems to networks, we require that any computer added to the House network have a supported version of AVG, Norton Anti-Virus or McAfee virus scan software installed and programmed to update at least weekly. Prior to connection on the network, all second computers must be thoroughly scanned by our staff to ensure they are virus free and all necessary operating system patches must be installed, which may take up to a few hours to complete. Upon successful scanning and updates, House Information

Systems staff will install security credentials on a computer that will allow a member to connect to the House network. Computers connected only to public wireless do not need to be scanned by House staff.

Additional computers are not covered under the House Clerk's Office licensing contracts. Therefore, members must purchase any desired software, such as Microsoft Office.

USE OF CAP PERSONAL COMPUTERS and TABLETS

Computer Use Policy Statements

- Users of the system must respect the privacy of other users and their intellectual property or data.
- Users shall not intentionally seek information, obtain copies, modify files or data, or use passwords belonging to other users without proper authorization.
- Users shall not represent themselves as another user, unless authorized to do so by that user.
- Users shall respect the legal protection provided by copyright and licensing laws to software and data.
- Users shall protect the integrity of the Legislature's computer system and shall not intentionally propagate programs and harass other users or infiltrate a computer or computer system.
- Users shall not damage or alter the software or other components of legislative computers or computer systems, or install unauthorized software or hardware peripherals.
- Users shall not sell access to computer systems.
- Users shall be responsible for damage to assigned computer equipment and software that results from negligence and/or improper use.

Authorized Users

Any member of the House of Delegates who has been assigned a computer, laptop or tablet for legislative purposes.

- Any person employed by the House of Delegates or authorized by a member to use that member's assigned computer for legislative purposes.

- Authorized users shall not have access to the internal wireless network via privately owned personal computers.

Appropriate Use

Members and their authorized user (s) are not restricted in the use of the assigned personal computer and associated equipment and installed software as long as the use promotes computer skills and does not interfere with or inhibit legislative functions.

An authorized user who accesses the Internet has an obligation to use this access in a responsible and informed way, conforming to network etiquette, customs, and courtesies.

Each user is individually responsible for the content of any communication sent over or placed on any House of Delegates, Senate of Virginia and/or General Assembly networks, and the Internet.

In order to maintain the security of legislative hardware and software, a user of the Internet may not download or install application software or freeware without prior authorization from the Chief Technology Officer or the Clerk of the House.

Examples of appropriate computer use for members and staff are:

- to facilitate communications between legislators, staff, state agencies, constituents, and others concerned with state business, including the transfer of documents and usage of electronic mail;

- to access databases and files to obtain reference material, conduct research, or other appropriate legislative business;
- to expedite administrative duties in direct support of legislative-related functions;
- compile information for bill drafting, committee hearings, and floor debate;
- to preserve historical information related to the General Assembly;
- to facilitate work as a citizen legislator.

Inappropriate Use

No legislator or legislative staff may misappropriate, misapply, convert, or misuse any property or thing of value belonging to the state or any state agency.

In addition, no person shall use legislative computers and computer systems to:

- violate any state or federal law or regulation, including raising funds or directly managing campaign activities;
- intentionally disrupt network or system use by others, by introducing viruses or by other means;
- misrepresent oneself, a state agency, the General Assembly, a legislator, a state employee, or the state (including unauthorized use of another's password or login code); or
- Knowingly transmit or receive pornographic material or material that is intended to coerce, threaten, intimidate, or harass another individual.

Security and Privacy

The General Assembly employs various measures to protect the security of its computing resources and its users' accounts. Users should be aware, however, that the General Assembly couldn't guarantee such security.

Users should also be aware that their uses of General Assembly computing resources are not completely private. While the General Assembly does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the legislature's computing resources require backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the rendition of service. The General Assembly may also specifically monitor the activity and accounts of individual users of legislative computing resources, including individual log in sessions and communications, without notice, when (a) the user has voluntarily made accessible to the public, as by posting to Usenet or a web page; (b) it reasonably appears necessary to do so to protect the integrity, security, or functionality of legislative or other computing resources or to protect the General Assembly from liability; (c) there is reasonable cause to believe the user has violated or is violating this policy; (d) an account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns; or (e) it is otherwise permitted or required by law. Any such individual monitoring, other than that specified in (a), required by law or necessary to respond to perceived emergency situations must be authorized in advance by the Clerk of the House or the Clerk of the Senate as appropriate.

The General Assembly may disclose the results of any such general or individual monitoring, including the contents of individual communications, to appropriate General Assembly officers or committees or to law enforcement

agencies and may use the results in appropriate proceedings. Communications made by means of General Assembly computing resources also may be subject to disclosure under the Commonwealth's Freedom of Information Act to the same extent as they would be if made on paper.

Electronic Mail and Internet Access

Members will have an electronic mail address which is posted on the Virginia General Assembly website. Each authorized user should use personal discretion in publicizing their personal email addresses.

It is important to remember that electronic mail and access to the Internet provide a valuable communications tool for legislators and legislative staff. As with all other forms of communication, these tools must be managed in a manner that maintains public trust and confidence in the General Assembly**.** One of the greatest distinctions, and dangers, of electronic mail and other forms of access to the Internet, is that people treat it far more informally than other forms of business communications. People can copy and circulate these communication resources far more easily than traditional paper documents.

Please note that any information entered by an authorized user may constitute a public record under §§ 2.2-3701 and 2.2-3704 of the Code of Virginia. Email accounts are maintained by users. The House of Delegates does not impose any size limits or expiration dates on a member's email account. However, deleted email expires from House of Delegates maintained backups after two years. Legislators and staff should use careful management so that electronic mail will constitute clear and appropriate communications.

Users acknowledge that use of electronic mail (e-mail) does not ensure privacy of their messages. Users also acknowledge that access to the Internet is not necessarily a private matter.

Ownership of Assigned Property

The hardware assigned to a member and the software installed in that hardware before assignment and subsequent upgrades to that software are property of the Virginia House of Delegates.

Maintenance and Support

The House of Delegates is responsible for providing reasonable maintenance and support of assigned personal computers and tablets, and installed/authorized hardware and software. If a member wishes to install additional software and/or hardware not specified in the authorized list, the member must contact the Chief Technology Officer of the Clerk of the House. It will be at the discretion of the Clerk to approve such installations, based on legitimate need and insuring that the installation does not negatively affect the primary function of the equipment.

An authorized user may not request the House of Delegates or their staff, or agents to provide training, installation service, or other support services for hardware or for software not installed by the House of Delegates or by the Clerk.

A member is responsible for the cost of repairing state-owned equipment or authorized software damaged as the result of negligence or abuse, or damaged through the installation of unauthorized equipment or software, including the cost of repairing any equipment or software adversely affected by the unauthorized hardware or software.

Prohibited Uses

An authorized user may not install software on assigned hardware, unless approved by the Chief Technology Officer or the Clerk. Users may not replace or attach hardware to assigned hardware without advance notice to and approval by the Chief Technology Office and the Clerk of the House of Delegates.

Users may not sell or provide to any other person any state-owned computer and associated hardware assigned to that user; sell, copy, provide to, or download for any other person any software loaded on or provided with assigned

computer equipment; or sell or provide any access to legislative information systems to which that user has been authorized or granted access.

Ramifications/Penalties

Upon notification to the Clerk of the House of Delegates regarding possible inappropriate use, the Speaker of the House of Delegates will be informed, or in the case of a member's staff, the Clerk shall advise the appropriate member.

The Rules Committees shall be responsible for the review of alleged violations of the policy agreement and shall discharge appropriate penalties, which may include termination of access privileges.

Notification if Hardware Damaged or Lost

The member shall notify the Chief technology Officer or the Clerk of the House as soon as possible after any damage to or loss of the assigned personal computer or associated hardware.

Liability for Use

The member assumes responsibility for any damage or loss resulting from misuse of equipment. The member is not responsible for any damage or loss resulting from complying with this policy.

House Information Systems shall arrange for repairs under any applicable warranty for their respective members.

Return of Hardware and Software

Hardware and associated equipment must be returned upon the death of the member, or upon the resignation or retirement of the member, as outlined in the Retiring Member policy. Upon recall of the hardware or software for replacement or trade-in of hardware, upgrade of software, or reassignment to another member, the hardware shall be returned to House Information Systems.